CLAIMS

What is claimed is:

1) A method for transmitting streaming data, comprising:

establishing a shared secret between a receiving participant and a sending participant;

using the shared secret to initialize a cryptographically secure hashed end of file marker for the streaming data;

transmitting the streaming data from the sending participant to the receiving participant; and

comparing the streaming data with the cryptographically secure hashed end of file marker to determine when an end of the streaming data occurs.

2) The method of claim 1 further comprising updating the cryptographically secure hashed end of file marker with contents of each block of the streaming data as the streaming data is transmitted.

3) The method of claim 2 wherein the hash function is SHA-1.

4) The method of claim 2 wherein the hash function is MD5.

5) The method of claim 1 further comprising:

calculating, by the receiving participant, the end of file marker, and

comparing, by the receiving participant, blocks of data within the streaming data with the end of file marker to determine if any data in the streaming data matches the end of file marker.

6) The method of claim 5 further comprising determining, by the receiving participant, that the end of the streaming data occurs when data in the streaming data matches the end of file marker.

7) The method of claim 6 further comprising determining, by the receiving participant, that the end of the streaming data does not occur as long as data in the streaming data does not match the end of file marker.

8) A computer-readable medium having computer-readable program code embodied therein for causing a computer system to perform:

exchanging a public key between two participants to generate a secret key;

initializing, with the secret key, a cryptographically secure end of file for streaming data;

streaming data between the two participants; and

transmitting the cryptographically secure end of file to signify between the participants an end to the streaming data.

9) The computer-readable medium of claim 8 for causing the computer system to further perform blocking, by at least one of the participants, data occurring after receipt of the cryptographically secure end of file.

10) The computer-readable medium of claim 8 for causing the computer system to further perform streaming data from a sending participant to a receiving participant with the receiving participant not knowing a length of the streaming data while streaming data between the two participants occurs.

11) The computer-readable medium of claim 8 wherein only the two participants can recognize the cryptographically secure end of file for the streaming data.

12) The computer-readable medium of claim 11 wherein the two participants include a sending participant that sends the streaming data and a receiving participant that receives the streaming data.

13) The computer-readable medium of claim 8 wherein initializing, with the secret key, the cryptographically secure end of file for streaming data further comprises combing a hash function with the secret key.

14) A system for transmitting streaming data, comprising:

a network;

a first participant in communication with the network; and

a second participant in communication with the network,

wherein the first and second participants communicate via the network to calculate a cryptographically secure end of file marker for the streaming data such that only the first and second participants can recognize the cryptographically secure end of file marker for the streaming data and such that cryptographically secure end of file marker is updated as the streaming data is transmitted or received.

15) The system of claim 14 wherein the receiving participant calculates the cryptographically secure end of file marker using both an asymmetric key exchange and a hash function.

16) The system of claim 15 wherein the asymmetric key exchange is Diffie-Hellmann and the hash function is SHA-1.

17) The system of claim 14 wherein the first and second participants communicate via the network to authenticate themselves so the participants are who they claim to be.

18) The system of claim 14 wherein only the end of file marker is cryptographically secured in the streaming data.

19) The system of claim 14 wherein the second participant automatically detects the cryptographically secure end of file marker, and the detection of the end of file marker, by the second participant, validates that the streaming data is not corrupted.

20) The system of claim 14 wherein the cryptographically secure end of file marker is calculated during transmission of the streaming data from the first participant to the second participant, and wherein the second participant automatically stops receiving data when the second participant determines that the cryptographically secure end of file marker is located in the streaming data.